RECEIVED
CENTRAL FAX CENTER
FEB 20 2007

AMENDMENTS TO THE CLAIMS

The following is a complete listing of the claims, which replaces all previous versions and listings of the claims.

1. (currently amended) A method of generating a ~~random number~~ cryptographic key for a cryptographic security subsystem of a processor-based device, the method comprising the acts of:

(a) detecting occurrence of a first type of triggering event;

(b) writing one or more bits of data to a seed pool upon termination of the first type of triggering event, the seed pool comprising a state bit indicative of a state of the seed pool;

(c) detecting occurrence of a second type of triggering event;

(d) writing one or more bits of data to the seed pool upon termination of the second type of triggering event, wherein act (d) comprises masking one or more bits of data to the seed pool upon termination of the second type of triggering event;

(e) examining the state bit to determine whether the seed pool is full; [[and]]

(f) if the seed pool is not full, repeating acts (a) through (e) until the seed pool is full[[.]]; and

(g) generating a pseudo-random number from the seed pool, wherein the pseudo-random number is used to generate the cryptographic key for the cryptographic security subsystem of the processor based device.

2. (canceled)

PAGE 5/29 * RCVD AT 2/20/2007 6:07:28 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/33 * DNIS:2738300 * CSID:281 970 4503 * DURATION (mm-ss):10-30

3. (original) The method as recited in claim 1, wherein the first type of triggering event has a variable duration.

4. (original) The method as recited in claim 1, wherein the processor-based device is coupled to a communication link, and wherein act (a) comprises the act of receiving a communication from the communication link.

5. (original) The method as recited in claim 4, wherein the communication link comprises a network.

6. (original) The method as recited in claim 4, wherein the communication link comprises the Internet.

7. (canceled)

8. (canceled)

9. (previously presented) The method as recited in claim 1, wherein act (d) comprises capturing the one or more bits of data from a free-running timer upon termination of the second type of triggering event.

10. (previously presented) The method as recited in claim 1, wherein the second type of triggering event is different than the first type of triggering event.

PAGE 6/29 * RCVD AT 2/20/2007 6:07:28 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/33 * DNIS:2738300 * CSID:281 970 4503 * DURATION (mm-ss):10-30

11. (previously presented) The method as recited in claim 1, wherein the second type of triggering event is a cycle of power applied to the processor-based device.

12. (canceled)

13. (currently amended) A method of initializing a seed pool for generating a ~~random number~~ cryptographic key for a cryptographic security subsystem of a processor-based device, the method comprising the acts of:

(a) prior to enabling the cryptographic security subsystem, writing a plurality of bits of data to a seed pool, the plurality of bits of data having a signature value;

(b) detecting occurrence of a first type of triggering event;

(c) writing one or more bits of data to the seed pool upon termination of the first type of triggering event, the one or more bits of data altering the signature value of the seed pool; [[and]]

(d) enabling the cryptographic security subsystem when more than a predetermined portion of the signature value of the seed pool has been altered[[.]]; and

(e) generating a pseudo-random number from the seed pool, wherein the pseudo-random number is used to generate the cryptographic key for the cryptographic security subsystem of the processor based device.

PAGE 7/29 * RCVD AT 2/20/2007 6:07:28 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/33 * DNIS:2738300 * CSID:281 970 4503 * DURATION (mm-ss):10-30

14. (original) The method as recited in claim 13, wherein the first type of triggering event comprises a cycle of power applied to the processor-based device.

15. (original) The method as recited in claim 13, wherein the first type of triggering event is a reboot of the processor-based device.

16. (original) The method as recited in claim 13, wherein act (c) comprises the act of masking the one or more bits of data into the seed pool.

17. (original) The method as recited in claim 13, wherein act (c) comprises the act of capturing the one of more bits of data from a free-running timer.

18. (original) The method as recited in claim 13, comprising the acts of:

detecting a second type of triggering event;

determining if the seed pool is full; and

writing one or more bits of data to the seed pool upon termination of the second type of triggering event if the seed pool is not full.

19. (previously presented) A processor-based device comprising:

a host processing system, the host processing system comprising a processor;

a communications management system in communication with the host processing system;

a memory system in communication with the host processing system and the communications management system,

PAGE 8/29 * RCVD AT 2/20/2007 6:07:28 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/33 * DNIS:2738300 * CSID:281 970 4503 * DURATION (mm-ss):10-30

wherein the communications management system comprises:

an interface controller;

a non-volatile memory device to store a seed pool, wherein the seed pool comprises a state bit indicative of the state of the seed pool; and

security logic in communication with the interface controller and the non-volatile memory device, the security logic configured to generate a cryptographic key to establish a secure communication session between the processor-based device and an external device in communication with the processor-based device via the interface controller, wherein the security logic generates the cryptographic key from the seed pool stored in the non-volatile memory device, and wherein the security logic is configured to:

detect occurrence of a first type of triggering event;

examine the state bit to determine whether the seed pool is fully populated;

write one or more bits of data to the seed pool upon termination of the first type of triggering event if the seed pool is not fully populated;

detect the occurrence of a second type of triggering event; and

mask one or more bits of data to the seed pool upon termination of the second type of triggering event.

20. (canceled)

PAGE 9/29 * RCVD AT 2/20/2007 6:07:28 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/33 * DNIS:2738300 * CSID:281 970 4503 * DURATION (mm-ss):10-30

21. (canceled)

22. (original) The processor-based device as recited in claim 19, wherein the first type of triggering event has a variable duration.

23. (original) The processor-based device as recited in claim 19, wherein the first type of triggering event comprises receipt, by the interface controller, of a communication from an external device.

24. (original) The processor-based device as recited in claim 23, wherein the interface controller comprises a network interface controller.

25. (original) The processor-based device as recited in claim 23, wherein the interface controller comprises an RS232 interface controller.

26. (previously presented) The processor-based device as recited in claim 19, wherein the processor-based device comprises a main power supply to supply power to the processor-based device, and wherein the second type of triggering event comprises a cycle of the power supplied by the main power supply.

27. (previously presented) A processor-based device comprising:

a host processing system, the host processing system comprising a processor;

a communications management system in communication with the host processing system; and

PAGE 10/29 * RCVD AT 2/20/2007 6:07:28 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/33 * DNIS:2738300 * CSID:281 970 4503 * DURATION (mm-ss):10-30

a memory system in communication with the host processing system and the communications management system,

wherein the communications management system comprises:

an interface controller;

a non-volatile memory device to store a seed pool comprising a plurality of data bits; and

security logic in communication with the interface controller and the non-volatile memory device, the security logic configured to establish a secure communication session between the processor-based device and an external device in communication with the processor-based device via the interface controller, and wherein the security logic is configured to:

write the one or more bits to the seed pool, the bits altering a signature value;

determine whether the plurality of data bits in the seed pool has at least a portion of the signature value; and

disable establishment of the secure communication session if the plurality of data bits has at least a portion of the signature value.

28. (canceled)

29. (previously presented) The processor-based device as recited in claim 27, comprising a main power supply to supply power to the processor-based device, and wherein

PAGE 11/29 * RCVD AT 2/20/2007 6:07:28 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/33 * DNIS:2738300 * CSID:281 970 4503 * DURATION (mm-ss):10-30

the first type of triggering event comprises a cycle of the power supplied by the main power supply.

30. (original) The processor-based device as recited in claim 27, wherein the security logic is configured to:

detect a second type of triggering event;

determine whether the seed pool is fully populated; and

write one or more data bits to the seed pool upon termination of the second type of triggering event if the seed pool is not fully populated.

31. (original) The processor-based device as recited in claim 30, wherein the second type of triggering event comprises receipt of a communication from the external device via the interface controller.

32. (original) The processor-based device as recited in claim 31, wherein the interface controller comprises a network interface controller.

33. (previously presented) The method as recited in claim 1, wherein act (b) comprises the act of capturing one or more bits of data from a free-running timer upon termination of the first type of triggering event.

34. (previously presented) The processor-based device as recited in claim 19, wherein the communications management system comprises a free-running timer, and

PAGE 12/29 * RCVD AT 2/20/2007 6:07:28 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/33 * DNIS:2738300 * CSID:281 970 4503 * DURATION (mm-ss):10-30

wherein the security logic is configured to capture the one or more bits of data from the free-running timer upon termination of the first type of triggering event.

35. (previously presented) The processor-based device as recited in claim 27, wherein the security logic is configured to detect a first type of triggering event, and to write one or more data bits to the seed pool upon termination of the first type of triggering event.

36. (previously presented) A method for restoring security data to non-volatile memory in a computer system comprising:

writing bits to a seed pool in discrete increments corresponding to a triggering event, wherein the seed pool is stored in a portion of a non-volatile memory device;

tracking the state of the seed pool to determine if the seed pool is fully populated; and

precluding access to the computer system if it is determined that the seed pool is not fully populated.

37. (previously presented) The method of claim 36 wherein the triggering event comprises receipt of a query from a device external to the computer system.

38. (previously presented) The method of claim 36 wherein writing bits to the seed pool in discrete increments corresponding to the triggering event comprises masking bits into the seed pool in discrete increments corresponding to a power cycle of the computer system.

PAGE 13/29 * RCVD AT 2/20/2007 6:07:28 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/33 * DNIS:2738300 * CSID:281 970 4503 * DURATION (mm-ss):10-30

39. (previously presented) The method of claim 36 wherein tracking the state of the seed pool comprises examining a state bit, wherein the state bit changes states when the seed pool is fully populated.

40. (previously presented) The method of claim 36 wherein tracking the state of the seed pool comprises examining the position of a pointer to determine whether the portion of the non-volatile memory storing the seed pool is full.

PAGE 14/29 * RCVD AT 2/20/2007 6:07:28 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/33 * DNIS:2738300 * CSID:281 970 4503 * DURATION (mm-ss):10-30